REMARKS

Applicant appreciates the Examiner's review of this application and respectfully requests reconsideration and allowance of the pending claims. Claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49,51-63, 65-77, and 79-81 are pending in this application.

Claim Amendments

Claims 1-82 were previously pending.

Amended claims: 1-7, 9-10, 12-22, 24-25, 27-28, 31-32, 35-36, 39-41, 44-49, 51-53, 58-63, 65-67, 70-77, and 79-81.

Canceled claims: 8, 11, 23, 26, 33, 34, 38, 50, 64, 78, and 82.

No new claims are added.

Pending claims: 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49,51-63, 65-77, and 79-81.

Rejection of the Claims

35 U.S.C. § 112, second paragraph

Claims 2, 17, and 32 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter set forth therein.

Claims 2, 17, and 32 have been amended to more particularly point out and distinctly claim the subject matter. "Data" has been amended to "data block" with antecedent basis in the base claims. The amendments do not narrow the claims. The specification describes "Data block D can contain any type of data, including logon data, various data files, permissions, etc." (page 9, lines 8-9 of the specification). Applicant respectfully submits that the 35 U.S.C. § 112, second paragraph rejections of claims 2, 17, and 32 are overcome with these amendments.

35 U.S.C. § 112, first paragraph

Claims 8, 11, 23, 26, 38, 41, 50, 53, 64, 67, 78, and 81 were rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement, i.e., as containing subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention.

Claims 8, 23, 38, 50, 64, and 78

In these claims, the Office rejects the language "generating at least a portion of the encryption key" "hashing at least a portion of the digitally signed second data" [string] and "at least a portion of the third data" [string] as not being described in the specification.

Applicant respectfully disagrees with the rejection and maintains that the rejected language is inherently described in the specification because those skilled in the relevant arts, such as cryptology and programming with string operators, will appreciate that encryption, hashing, and other operations performed on data strings are commonly performed on only part of a data string and need not always be performed on entire data string to have effect.

Nonetheless, the rejected claims have been canceled, so the rejection is moot. The subject matter of claims 8, 23, 38, 50, 64, and 78 and the rejected language is included explicitly or inherently in other pending claims.

Claims 11, 26, 41, 53, 67, and 81

In these claims, the Office rejects the language "substantially randomly generated" as not being described in the specification.

Applicant respectfully disagrees with the rejection and maintains that the rejected language is inherently described in the specification because those skilled in the art of random number generation understand that a truly random number or sequence of random numbers is difficult or impossible to produce, whereas the phrase "substantially random" encompasses random numbers and pseudo random numbers as used in common parlance.

Nonetheless, Applicant requests the cancellation of claims 11 and 26 without prejudice since their subject matter is found in other claims. Applicant also amends claims 41, 53, 76, and 81 to delete the word "substantial." Applicant respectfully submits that the 35 U.S.C. § 112, first paragraph rejections of claims 41, 53, 67, and 81 are overcome with this amendment.

Rejections under 35 USC § 102(b)

The Patent Office rejected claims 1-11, 13-26, 28-41 and 43 under USC § 102(b) as being anticipated by U.S. Patent No. 6,079,018 to Hardy et al. ("the Hardy reference" or "Hardy"). Applicant respectfully traverses these rejections.

Hardy does not expressly or inherently describe each element of claim 1.

In the MPEP § 2131, anticipation under 35 U.S.C. § 102 requires that:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Claim 1

Applicant's claim 1 as amended defines a method of:

generating first and second random values to allow a signature-generating process to encrypt and decrypt a data block;
digitally signing a first string, wherein the first string includes the first random value; and
generating an encryption key for encrypting the data block by hashing a combination of the digitally signed first string and the second random value.

Claim 1 is amended to more particularly point out and distinctly claim aspects of the subject matter, i.e., claim 1 is reorganized for clarity. The element of hashing a first string has been moved to dependent claim 3, wherein the first string is re-identified as a third random value. Moving this element broadens claim 1. No new matter has been added to the application.

In applicant's claim 1 as amended, a string is digitally signed and the digitally signed string is used to generate an encryption key for encrypting a data block.

In contrast, the Hardy reference is directed to a "system and method for generating unique secure values for digitally *signing* documents" (c.f., title of the Hardy reference). The Hardy reference provides a pseudo-random key for use in a digital *signature procedure* that is reliably distinct for every different document signed using the digital signature procedure (col. 7, lines 48-52). Hardy is particularly directed to reliably generating a distinct value for the pseudo-random key for each distinct document to be digitally *signed* and for ensuring that the pseudo-random key is as unguessable as the private key being used to *sign* the document (col. 1, lines 9-14).

However, although Hardy discloses a method of generating a reliable pseudo-random key for use in a digital *signature procedure*, and even discusses encrypting the private key and the pseudo-random key "k" used in the *signature process* for added security (col. 9, lines 36-39) Hardy does not disclose using a *signed* data string resulting from the Hardy *signature* process to generate an encryption key for encrypting a data block, as Applicant does. In other words, Hardy achieves a digital *signature* process and then stops, whereas Applicant uses the *results* of a *signature* process to generate an encryption key for encrypting a data block that may be unrelated to the *signature* process.

Since Hardy does not disclose Applicant's element of using a signed string to generate an encryption key for encrypting a data block, Applicant respectfully traverses the rejection, and respectfully submits that claim 1 is patentable over the Hardy reference.

Claims 2-7, 9-10, and 13-15

For at least the reasons set forth above with respect to claim 1, Applicant submits that claims 2-7, 9-10, and 13-15 are patentable over the Hardy reference. Dependent claims contain the language of the claims from which they depend. Claims 2-7, 9-10, and 13-15 depend directly or indirectly from claim 1. Claim 1 is allowable, therefore, claims 2-7, 9-10, and 13-15 are also allowable.

Claims 3 and 4 define the method of claim 1, further including the option of generating a third random value and including the third random value and its hash in a data block to be encrypted as in the method of base claim 1. After encryption, when the data block is later decrypted, the decrypted third random value and the decrypted hash of the third random value can be compared with a new hash of the decrypted third random value. In this way, the decryption key can be verified by comparing the new hash of the decrypted third random value with the decrypted (former) hash of the third random value.

Since Hardy does not disclose Applicant's elements of including values and hash values in the data block to be encrypted and using these included values and hash values as a verification measure for the decryption key, Applicant respectfully submits that claims 3 and 4 are further patentable over the Hardy reference over and above the reasons stated above.

Claim 16

Claim 16 is amended to more particularly point out and distinctly claim aspects of the subject matter, that is, claim 16 is reorganized for clarity. The element of hashing a first string has been moved to dependent claim 18, wherein the first string is re-identified as a third random value. Moving this element broadens claim 16. No new matter has been added to the application.

Similar to claim 1, claim 16 includes a feature of generating an encryption key for encrypting a data block based on a digitally signed string and a second random value. For at least the reasons discussed above for claim 1, Hardy does not disclose Applicant's element of using a signed string to generate an encryption key for encrypting a data block. Applicant respectfully traverses the rejection, and respectfully submits that claim 16 is patentable over the Hardy reference.

Claims 17-22, 24-25, and 28-30

For at least the reasons set forth above with respect to claim 16, Applicant submits that claims 17-22, 24-25, and 28-30 are patentable over the Hardy reference. Dependent claims contain the language of the claims from which they depend. Claims 17-22, 24-25, and 28-30 depend directly or indirectly from claim 16. Claim 16 is allowable, therefore claims 17-22, 24-25, and 28-30 are also allowable.

Claims 18 and 19 define the method of claim 1 further including the option of generating a third random value and including the third random value and its hash in a data block to be encrypted as in the method of base claim 16. After encryption, when the data block is later decrypted, the decrypted third random value and the decrypted hash of the third random value can be compared with a new hash of the decrypted third random value. In this way, the decryption key can be verified by comparing the new hash of the decrypted third random value with the decrypted (former) hash of the third random value.

Since Hardy does not disclose Applicant's elements of including values and hash values in the data block to be encrypted and using these included values and hash values as a verification measure for the decryption key, Applicant respectfully submits that claims 18 and 19 are further patentable over the Hardy reference over and above the reasons stated above.

Claim 31

Similar to claim 1, claim 31 includes logic configured to generate an encryption key based on a combination of a digitally signed data string and another data string. For at least the reasons discussed above for claim 1, Hardy does not disclose Applicant's element of using a signed string to generate an encryption key for encrypting a data block. Applicant respectfully traverses the rejection, and respectfully submits that claim 31 is patentable over the Hardy reference.

Claims 32, 35-37, 39-41, and 43

For at least the reasons set forth above with respect to claim 31, Applicant submits that claims 32, 35-37, 39-41, and 43 are patentable over the Hardy reference. Dependent claims contain the language of the claims from which they depend. Claims 32, 35-37, 39-41, and 43 depend directly or indirectly from claim 31. Claim 31 is allowable, therefore claims 32, 35-37, 39-41, and 43 are also allowable.

35 U.S.C. § 103(a)

Claims 12-15, 27-29, and 42-82 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the Hardy reference in view of U.S. Patent No. 6,453, 416 to Epstein ("the Epstein reference" or "Epstein"). Applicant respectfully traverses these rejections.

The Patent Office Has Not Established A Prima Facie Case Of Obviousness Under 35 U.S.C. § 103(a)

To establish a prima facie case of obviousness, the prior art references, when combined, must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Claims 12-15

Claims 12-15 depend directly or indirectly from claim 1 and include all the language of claim 1. The Hardy reference describes generating unguessable pseudo-random keys "k" used for added security in the *signature process* (col. 9, lines 36-39). Hardy does not teach or suggest using a *signed* data string resulting from the Hardy *signature* process to generate an encryption key for encrypting a data block, as does Applicant's claims 12-15.

The combination of Hardy and Epstein fails to produce an obviousness rejection for claims 12-15.

The Epstein reference describes a secure proxy signing device, which merely encrypts a hash of a document with a private key to form the digital *signature* if the hash of the document has been authenticated (e.g., col. 2, lines 40-48). The Epstein reference does not teach or suggest claims 12-15's element of generating an encryption key for encrypting a data block from a digitally signed string, and when combined with the Hardy reference does not cure the missing teaching in Hardy to produce Applicant's feature of generating an encryption key for encrypting a data block from a digitally signed string. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claims 12-15.

Applicant respectfully requests that the obviousness rejection be removed from claims 12-15 and earnestly seeks their allowance.

Claims 27-29

Claims 27-29 depend directly or indirectly from claim 16, and include all the language of claim 16. Claim 16 recites a computer readable medium that includes instructions for generating an encryption key for encrypting a data block based on a digitally signed string and a second random value. Neither the Hardy reference nor the Epstein reference, alone or in combination, teach or suggest claims 27-29's element of generating an encryption key for encrypting a data block from a digitally signed string. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claims 27-29.

Applicant respectfully requests that the obviousness rejection be removed from claims 27-29 and earnestly seeks their allowance.

Claims 42-43

Claims 42-43 depend from claim 31, and include all the language of claim 31. Claim 31 recites an arrangement that includes and element of generating an encryption key for encrypting a data block based on a digitally signed string and another string. Neither the Hardy reference nor the Epstein reference, alone or in combination, teach or suggest claims 42-43's element of generating an encryption key for encrypting a data block from a digitally signed string. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claims 42-43.

Applicant respectfully requests that the obviousness rejection be removed from claims 42-43 and earnestly seeks their allowance.

Claims 44-49 and 51-57

Claim 44 recites a method that includes an element of generating an encryption key for encrypting a data block based on a digitally signed string and another string. Claims 45-49 and 51-57 depend from claim 44 and include all the language of claim 44. Neither the Hardy reference nor the Epstein reference, alone or in combination, teach or suggest the element in claims 44-49 and 51-57 of generating an encryption key for encrypting a data block from a digitally signed string. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claims 44-49, and 51-57.

Applicant respectfully requests that the obviousness rejection be removed from claims 44-49, and 51-57 and earnestly seeks their allowance.

Claims 58-63 and 65-71

Claim 58 recites a computer readable medium that includes instructions for generating an encryption key for encrypting a data block based on a digitally signed string and another string. Claims 59-63 and 65-71 depend from claim 58 and include all the language of claim 58. Neither the Hardy reference nor the Epstein reference, alone or in combination, teach or suggest the element in claims 58-63 and 65-71 of generating an encryption key for encrypting a data block from a digitally signed string. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claims 58-63, 65-71.

Applicant respectfully requests that the obviousness rejection be removed from claims 58-63, 65-71 and earnestly seeks their allowance.

Claims 72-77 and 79-81

Claim 72 recites a system that includes logic for generating an encryption key for encrypting a data block based on a digitally signed string and another string. Claims 73-77 and 79-81 depend from claim 72 and include all the language of claim 72. Neither the Hardy reference nor the Epstein reference, alone or in combination, teach or suggest the element in claims 72-77 and 79-81 of generating an encryption key for encrypting a data block from a digitally signed string. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claims 72-77 and 79-81.

Applicant respectfully requests that the obviousness rejection be removed from claims 72-77 and 79-81 and earnestly seeks their allowance.

CONCLUSION

Applicant respectfully suggests that claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81 are in condition for allowance and requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 8-13-04

By:

Lee & Hayes PLLC
Mark C. Farrell
Reg. No. 45,988
(509) 324-9256